PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00 // H04Q 2 /38, H04L 9 /32 — A1

(11) International Publication Number: WO 99/10793

(43) International Publication Date: 4 March 1999 (04.03.99)

(21) International Application Number: PCT/FI98/00653

(22) International Filing Date: 25 August 1998 (25.08.98)

(30) Priority Data:
973528 27 August 1997 (27.08.97) FI

(71) Applicant *(for all designated States except US)*: SONERA OY [FI/FI]; Sturenkatu 16, FIN–00510 Helsinki (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: LINKOLA, Janne [FI/FI]; Kuusikallionkuja 4 F 43, FIN–02210 Espoo (FI). HOKKANEN, Tuomo [FI/FI]; Strömsinlahdenkuja 2 A 13, FIN–00820 Helsinki (FI).

(74) Agent: PAPULA REIN LAHTELA OY; Fredrikinkatu 61 A, P.O. Box 981, FIN–00101 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: PROCEDURE FOR ACCESSING A SERVICE IN A DATA COMMUNICATION SYSTEM, AND A DATA COMMUNICATION SYSTEM

(57) Abstract

The invention relates to a procedure and a data communication system in which a service provider gives the user of a service a set of expendable passwords that the user can use to access the service via a telecommunication and/or data network. The system comprises a user's terminal device provided with means for sending a password at log–on to the service, and a server to which the terminal device sets up a connection and which comprises means for identifying the password and for allowing/denying access to the service on the basis of the password supplied. The terminal device comprises means for storing a set of passwords and for selecting the right password from the stored set of passwords at log–on to a predetermined service to allow automatic addition of the password to a connection setup signal to be transmitted from the terminal device to the server.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

PROCEDURE FOR ACCESSING A SERVICE IN A DATA COMMUNICATION SYSTEM, AND A DATA COMMUNICATION SYSTEM

The present invention relates to a procedure as defined in the preamble of claim 1. Moreover, the invention relates to a system as defined in the preamble of claim 6.

Reliable user identification is a prerequisite for the use of many services provided in the general telecommunication network or in other data networks. Such services include e.g. bank services. The service may involve significant economic effects and therefore the service provider wants to ascertain the user's identity before making the service available.

Very often, e.g. in conjunction with bank services, the user is identified by means of passwords. Usually these passwords are expendable. The service provider or an identifying party authorised by the service provider has given the user beforehand a number of passwords (e.g. four-digit numbers), one of which the customer uses each time he/she needs the services. When a list of passwords is about to be exhausted, the service provider (or a party authorised by the service provider) sends the user a new list of passwords. Thus, the user always has a sufficient number of passwords for his/her needs in the near future.

A feature typical of prior-art solutions is that the customer has to manually input an expendable password when logging on to a server. Often the password is entered by pressing the keys of a telephone set, causing the data to be transmitted to the server using tone frequency transmission, so-called DTMF (dual tone multifrequency) codes. In addition, there are many other methods for transmitting a password, such as the short-message service in the GSM network (GSM, Global System for Mobile Communications; in the present description, GSM network refers to any mobile communication system based on the GSM specifications).

However, the essential point is that the user has to manually input the password him/herself. This is in many cases quite difficult for the user.

Another feature typical of prior-art solutions is that the service provider must send a new set of passwords by using a rather unreliable transmission mechanism. The most commonly used method is to send them by mail. The problem is that the letter containing the passwords may end up in the wrong hands.

The object of the present invention is to eliminate the problems described above.

A specific object of the present invention is to disclose a completely new type of procedure and system for transmitting passwords between a user's telephone apparatus and a server.

A further object of the invention is to facilitate the use of services requiring passwords by reducing the number of routines necessitating user interaction in conjunction with the use of the services without making any compromises in regard of safety of the services.

The procedure of the invention is characterised by what is presented in claim 1. The system of the invention is characterised by what is presented in claim 6.

In the procedure of the invention for accessing a service in a data communication system, in which the service provider gives the user of a service a number of expendable passwords by means of which the user can access the service via a telecommunication and/or data network, a connection is set up from a terminal device to a server and a password is sent at log-on to the service, the password is identified and access to the service is allowed and/or denied based on the password supplied.

According to the invention, in the procedure, a set of passwords are stored in the terminal device,

the right password is selected from the stored set of passwords at log-on to a predetermined service, and the password is automatically added to a connection setup signal to be transmitted from the terminal device to the server.

Correspondingly, in the system of the invention, the terminal device comprises means for storing a set of passwords and selecting the right password from the stored set of passwords at log-on to a predetermined service to allow automatic addition of the password to a connection setup signal to be transmitted from the terminal device to the server.

The invention has the advantage that it discloses a completely new type of mechanism for the transmission of passwords between a user's telephone apparatus and a server. A further advantage of the invention is that it facilitates the use of services requiring passwords by reducing the number of routines necessitating user interaction in conjunction with the use of the services. This is done without any compromises regarding the safety of the services.

In an embodiment of the procedure, the used ones of the passwords in a set of passwords are registered.

In an embodiment of the procedure, the set of passwords in the terminal device is updated from the server via the telecommunication and/or data network.

In an embodiment of the procedure, an order for a new set of passwords is automatically sent to the server once the previous set of passwords has been exhausted.

In an embodiment of the procedure, several sets of passwords corresponding to different services are stored in the terminal device, and in connection setup the set of passwords corresponding to the service to be accessed in each case is selected.

In an embodiment of the system, the terminal device comprises means for registering the used ones of the passwords in a set of passwords.

In an embodiment of the system, the server comprises means for updating the set of passwords in the terminal device via a telecommunication and/or data network, and the terminal device comprises means for receiving a set of passwords.

In an embodiment of the system, the terminal device comprises means for automatic ordering of a new set of passwords from the server after the previous set of passwords has been exhausted.

In an embodiment of the system, the terminal device comprises means for storing several sets of passwords corresponding to different services.

In an embodiment of the system, the terminal device comprises means for selecting the set of passwords corresponding to the service to be used in each case.

In an embodiment of the system, the data communication system comprises a wired network and the terminal device is a telecommunication terminal, such as a telephone, in the wired network.

In an embodiment of the system, the data communication system comprises a mobile communication network, such as a GSM network, and the terminal device is a mobile station, such as a GSM telephone.

In an embodiment of the system, the terminal device is a GSM telephone, and the means for using said password management functions are disposed in a subscriber identity module, such as a SIM card.

In an embodiment of the system, in the connection setup between the subscriber identity module and the server, the transmission of passwords is effected by making use of the called subscriber number.

In an embodiment of the system, the software means of the subscriber identity module are designed

to identify the service on the basis of its identifier data, such as the telephone number, and to add a number of additional digits forming a password to the end of the telephone number of the service during call setup.

In an embodiment of the system, the subscriber identity module is provided with a service directory containing information specifying the services, the service identifier data and the names of the password files to be used in conjunction with the services.

In an embodiment of the system, the service directory is provided with a pointer for each service, which pointer has been arranged to point to the first unused password in the set of passwords and, after the password has been used, to move on to point to the next unused password in sequence.

In an embodiment of the system, the means for ordering new passwords and transmitting them between the server and the subscriber identity module comprise the short-message service (SMS-PP service) of the GSM network.

In the following, the invention will be described in detail by the aid of an application example.

The invention is based on providing the telephone apparatus with an extra module (physical or logical) allowing a functionality which creates additional signals in the communication between the telephone apparatus and the server in conjunction with a connection setup related to a service and/or additional fields and/or components or equivalent in the communication between the telephone apparatus and the server, the expendable password being transmitted in these additional signals/fields/components. This is done automatically without the user becoming aware of it. The module registers the passwords used each time

and therefore always knows which is the correct password to be used at log-on. The user will find this type of services easier to use, but in respect of data security they are of the same level with services in which the user must input the passwords him/herself. The extra module is also able to receive new passwords from the server and it can even order new passwords when necessary.

The extra module in the telephone apparatus may support simultaneous services requiring expendable passwords. For this purpose, the extra module contains a directory of services supported (in short, a service directory), which is used to identify a service requiring expendable passwords and to find the correct list of passwords and also to find the correct position in the list.

The best embodiment of the invention is a mobile station, such as a GSM telephone, whose subscriber identity module contains an application that uses SIM Application Toolkit commands to accomplish the extra functionality described above. The password transmission mechanism used in conjunction with the setup of a service connection between the SIM card and the server consists of the use of the called subscriber number, i.e. the so-called B-identifier. The application on the SIM card uses the `Call Control by SIM' command as defined in the TS GSM 11.14 specification, and in practice the application processes each called subscriber number, in other words, it compares the called subscriber number with the numbers stored in the service directory, and when it detects that the call is addressed to one of the stored numbers, it appends to the end of the telephone number a required number of additional digits in which the expendable password is encoded. For example, when the user is making a call to the number 0800-XYZ-123456, the application on the SIM card will change the number to

the form 0800-XYZ-123456-KLMN. The last four digits (KLMN) of the modified number are the expendable password added by the SIM card.

The service directory may be implemented as a special file on the SIM card. The special file contains information specifying the services supported, their identifier data and the names of the password files to be used in conjunction with the services. Moreover, for each service, the service directory contains a pointer that points to the current position in the list of passwords. Table 1 presents an example of the information elements contained in the special file.

For example, service 1 is identified from the fact that the user is calling the number 0800123. The application knows that it has to append to the end of the number an expendable password, which is found in the file 2FF5. In this instance, the password to be used is the thirteenth one in this file.

Service identifier	Method	Identifiers associated with method	Name of password file	Pointer	Total number of passwords
1	BID	0800123	2FF5	13	100
2	BID	0800456	2FF4	11	100
3	SMS	SMSC:+02 0202800 BID:8756	2FF6	2	9

Table 1. Service directory as used in an embodiment of the invention.

The server in the public telecommunication network receives the expendable password in the signalling in the telephone network. The server takes the last four digits of the B-identifier and assumes that they constitute an expendable password. The server

compares the expendable password thus obtained with its own information as to the user's next password. This is done by methods already known at present.

If the service requires the use of a user name at log-on to the service, the service directory may contain stored user names for each service. The user name can be appended to the connection setup signal in the same way as the password.

For the transmission of new passwords between the server and the application of the invention on the SIM card, it is possible to use the SMS-PP service of the GSM network. If the SIM card sends an order for new passwords, this is effected using the SMS-PP/MO (Mobile Originated) service and the passwords are transmitted to the SIM card using the SMS/PP-MT service.

The functionality of the application is divided between three blocks. The first block, an appending block, recognises the need to add an expendable password and sends a request to find the password to a password search block. Once the search block has found the right password, the appending block appends the expendable password it has received to the B-identifier and allows the call to proceed further from the telephone apparatus.

In the best embodiment of the invention, a block for adding new passwords works completely independently of the other blocks. In practice, it monitors the SMS Data Download traffic consistent with TS GSM 11.14 version 5.1.0 received by the SIM card and detects the appearance of new passwords on the card. The block for adding new passwords stores the new passwords received in the SMS Data Download message to a suitable special file on the SIM card and makes an appropriate addition to the service directory so that the search block will be able to find the new passwords. This new password file may be a combination

that contains the last unused passwords of the previous file and the completely new passwords just received.

The invention is not restricted to the application example described above, but many variations are possible within the scope of the inventive idea defined by the claims.

CLAIMS

1. Procedure for accessing a service in a data communication system, in which the user of the service is given a set of expendable passwords that the user can use to access the service via a telecommunication and/or data network, and in which procedure a terminal device is used to set up a connection to a server and a password is sent at log-on to the service, the password is identified and access to the service is allowed/denied based on the password supplied, characterised in that

a set of passwords is stored in the terminal device,

the right password is selected from the stored set of passwords at log-on to a predetermined service, and

the password is automatically added to a connection setup signal to be transmitted from the terminal device to the server.

2. Procedure as defined in claim 1, characterised in that the used ones of the passwords in a set of passwords are registered.

3. Procedure as defined in claim 1 or 2, characterised in that the set of passwords in the terminal device is updated from the server via the telecommunication and/or data network.

4. Procedure as defined in any one of claims 1 - 3, characterised in that an order for a new set of passwords is automatically sent to the server once the preceding set of passwords has been exhausted.

5. Procedure as defined in any one of claims 1 - 4, characterised in that several sets of passwords corresponding to different services are stored in the terminal device and, during connection setup, the set of passwords corresponding to the service to be accessed in each case is selected.

6. Data communication system in which the user of a service is given a set of expendable passwords that the user can use to access the service via a telecommunication and/or data network, said system comprising

- a user's terminal device provided with means for sending a password at log-on to the service,

- a server to which the terminal device sets up a connection, said server comprising means for identifying the password and for allowing/denying access to the service on the basis of the password supplied, characterised in that the terminal device comprises means for storing a set of passwords and selecting the right password from the stored set of passwords at log-on to a predetermined service to allow automatic addition of the password to a connection setup signal to be transmitted from the terminal device to the server.

7. System as defined in claim 6, characterised in that the terminal device comprises means for registering the used ones of the passwords in the set of passwords.

8. System as defined in claim 6 or 7, characterised in that the server comprises means for updating the set of passwords in the terminal device via the telecommunication and/or data network, and that the terminal device comprises means for receiving a set of passwords.

9. System as defined in any one of claims 6 - 8, characterised in that the terminal device comprises means for automatic ordering of a new set of passwords from the server after the previous set of passwords has been exhausted.

10. System as defined in any one of claims 6 - 9, characterised in that the terminal device comprises means for storing several sets of passwords corresponding to different services.

11. System as defined in claim 10, characterised in that the terminal device comprises means for selecting the set of passwords corresponding to the service to be used in each case.

12. System as defined in any one of claims 6 - 11, characterised in that the data communication system comprises a wired network and the terminal device is a telecommunication terminal, such as a telephone, in the wired network.

13. System as defined in any one of claims 6 - 12, characterised in that the data communication system comprises a mobile communication network, such as a GSM network, and the terminal device is a mobile station, such as a GSM telephone.

14. System as defined in any one of claims 13, characterised in that the terminal device is a GSM telephone, and that the means for using said password management functions are disposed in a subscriber identity module, such as a SIM card.

15. System as defined in claim 14, characterised in that, in the connection setup between the subscriber identity module and the server, the transmission of passwords is effected by making use of the called subscriber number.

16. System as defined in claim 14 or 15, characterised in that the software means of the subscriber identity module are designed to identify the service on the basis of its identifier data, such as the telephone number, and to append a number of additional digits forming a password to the end of the telephone number of the service during call setup.

17. System as defined in any one of claims 13 - 16, characterised in that the subscriber identity module is provided with a service directory containing information specifying the services, the service identifier data and the names of the password files to be used in conjunction with the services.

18. System as defined in claim 17, characterised in that the service directory is provided with a pointer for each service, which pointer has been arranged to point to the first unused password in the set of passwords and, after this password has been used, to move on to point to the next unused password in sequence.

19. System as defined in any one of claims 13 - 18, characterised in that the means for ordering new passwords and transmitting them between the server and the subscriber identity module comprise the short-message service (SMS-PP service) of the GSM network.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 98/00653

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 1/00 // H04Q 2/38, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

DIALO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FI 960820 (NOKIA MOBILE PHONES LTD.), 23 February 1996 (23.02.96), page 1 - page 3, abstract --	1-19
P,X	WO 9731306 A1 (NOKIA MOBILE PHONES LTD), 28 August 1997 (28.08.97), page 1 - page 3, abstract --	1-19
E,X	US 5812764 A (MICHAEL WILLIAM HEINZ), 22 Sept 1998 (22.09.98), column 2, line 55 - column 3, line 40; column 6, line 30 - column 7, line 10, figure 2, abstract --	1-19

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 February 1999	08 -02- 1999
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Authorized officer Linus Wretblad Telephone No. + 46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)